Remarks/Arguments

The Applicants respectfully request further examination and reconsideration in view of the amendments made above and the arguments set forth below. Claims 1-45, 47-52, and 59-73 were pending. Claims 46 and 53-58 were previously canceled. Within the Office Action, Claims 1-15, 19-24, 26-39, 42-45, 47-52, 59-69, and 72 have been rejected under 35 U.S.C. § 103(a); Claims 70, 71, and 73 have been allowed; and Claims 16-18, 25, 40, and 41 have been objected to. By way of the above amendments, Claims 1, 16, 17, 25, 26, 36, 40, 48, 71, and 73 have been amended, and new Claims 74 and 75 have been added. Accordingly, Claims 1-45, 47-52 and 59-75 are now pending.

Rejections under 35 U.S.C. § 103(a)

Claims 1-5, 11, 12, 19, 20, 26-28, 31, 36, 37, 39, 42, 43, 48-50, 61-69, and 72

Within the Office Action, Claims 1-5, 11, 12, 19, 20, 26-28, 31, 36, 37, 39, 42, 43, 48-50, 61-69, and 72 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,313,694 to Riedel ("Riedel") in view of Yu et al., "A Cryptographic File System Supporting Multi-Level Security" ("Yu"). The Applicants respectfully disagree.

Riedel is directed to securing file access via directory encryption. Riedel discloses encrypting filenames to protect them when a server is untrustworthy, such as in a distributed computing environment. Riedel also discloses encrypting filenames in a directory structure without otherwise changing the directory structure. (Riedel, Abstract)

Yu is directed to sharing encrypted files among multiple users. Yu discloses assigning an encryption key to each mandatory access control (MAC) class and assigning the same key to users within the same MAC class. (Yu at 3, second full paragraph)

Claim 1 is directed to a computer system comprising a memory portion containing an encrypted data file and an operating system comprising a kernel to use system-unique data to verify a user to control access to the encrypted data file, wherein the kernel comprises a virtual node (a) to decrypt an encrypted directory entry to determine a location of the encrypted data file and (b) to decrypt the encrypted data file to access data file contents contained therein.

Neither Riedel nor Yu, either alone or in combination, discloses the combination recited in Claim 1, including an operating system comprising a kernel to use system-unique data to verify a user to control access to the encrypted data file. For at least these reasons, the independent Claim 1 is allowable over Riedel, Yu, and their combination.

The limitation added to Claim 1 finds support throughout the application. A kernel using system unique data to verify a user and thus control access to an encrypted data file finds support at, for example, page 29, lines 4-10 (describing using system-dependent information such as a media access controller (MAC) identifier to verify a user), and page 53, lines 6-18 (describing using user identifiers and MAC as part of a credentials structure) of the Present Specification.

Claims 2-5, 11, 12, 19, 20, 61, 62, and 72 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable over Riedel, Yu, and their combination. Accordingly, Claims 2-5, 11, 12, 19, 20, 61, 62, and 72 are all also allowable as depending on an allowable base claim.

Claim 72 is allowable for at least one additional reason. Claim 72 incorporates from Claim 1 and thus recites a virtual node to decrypt an encrypted directory entry to determine a location of an encrypted data file. A plurality of different encryption keys encrypt different blocks of the data file. In contrast, Riedel discloses encrypting different directory entries with different keys. (Riedel, col. 4, lines 30-55) Even if the directory entries of Riedel could be considered data, Riedel does not disclose encrypted entries to determine a location of that data, as recited in Claim 72. In other words, Riedel does not disclose storing encrypted information for locating the directory entries. For this additional reason, Claim 72 is allowable.

The independent Claim 26 is directed to a computer system comprising a first device, a key generator, and a second device. The first device has an operating system kernel and a directory structure with directory information comprising encrypted data file names and corresponding encrypted data file locations for accessing encrypted data files within a file system, the operating system kernel to decrypt the encrypted data file names and encrypted data file locations using one or more encryption keys to recover clear data corresponding to the data file names, data file locations, and data files, the operating system kernel comprising a virtual node to encrypt the clear data using the one or more encryption keys to generate cipher data corresponding to the directory information and encrypted data files. The key generator is to generate the one or more encryption keys from identifiers unique to the computer system and unique to encrypted data files on the computer system. The second device is coupled to the first device to exchange cipher data with the first device. Neither Riedel nor Yu, either alone or in

combination, discloses the combination recited in Claim 26, including a key generator to generate one or more encryption keys from identifiers unique to the computer system and unique to encrypted data files on the computer system. For at least these reasons, the independent Claim 26 is allowable over Riedel, Yu, and their combination.

The limitation added to Claim 26 finds support throughout the application. A key generator to generate one or more encryption keys from identifiers unique to a computer system and unique to encrypted data files on the computer system finds support at, for example, page 20, lines 23-25 (discussing system to generate keys), and page 64, lines 1-8 (discussing an algorithm) of the Present Specification.

Claims 27, 28, 31, and 63-65 all depend on the independent Claim 26. As explained above, the independent Claim 26 is allowable over Riedel, Yu, and their combination. Accordingly, Claims 27, 28, 31, and 63-65 are all also allowable as depending on an allowable base claim.

The independent Claim 36 is directed to a method of storing an encrypted data file in a computer file system having a directory. The method of Claim 36 comprises receiving a clear data file having a name and executing kernel code in an operating system, the kernel code comprising a virtual node comprising drivers to encrypt the clear data file to generate an encrypted data file using a symmetric key, store the encrypted data file at a location in the computer file system, and store in the directory an entry containing an encryption of the name and an encryption of the location, wherein the symmetric key is generated in part by dividing a first key into sub-keys each corresponding to a block of the data file, modifying each of the sub-keys based on an identifier of a corresponding block to produce modified sub-keys, and combining the modified sub-keys. Neither Riedel nor Yu, either alone or in combination, discloses the combination recited in Claim 36, including using a symmetric key to encrypt a data file, where the symmetric key is generated in part by dividing a first key into sub-keys each corresponding to a block of the data file, modifying each of the sub-keys based on an identifier of a corresponding block to produce modified sub-keys, and combining the modified sub-keys. For at least these reasons, the independent Claim 36 is allowable over Riedel, Yu, and their combination.

The limitation added to Claim 36 finds support throughout the application. A symmetric key generated in part by dividing a first key into sub-keys each corresponding to a block of a data

file, modifying each of the sub-keys based on an identifier of a corresponding block to produce modified sub-keys, and combining the modified sub-keys, finds support at, for example, page 65, lines 4-16 of the Present Specification.

Claims 37, 39, 42, 43, 66, and 67 all depend on the independent Claim 36. As explained above, the independent Claim 36 is allowable over Riedel, Yu, and their combination. Accordingly, Claims 37, 39, 42, 43, 66, and 67 are all also allowable as depending on an allowable base claim.

The independent Claim 48 is directed to a computer system comprising a processor, a physical memory containing an encrypted data file and a directory, a secondary device coupled to the physical memory, and an operating system. The directory comprises a record having a first element corresponding to an encrypted name of the data file and a second element corresponding to an encrypted location of the data file in the memory. The operating system comprises a kernel, the kernel comprising a virtual node integrated with drivers to directly decrypt the first and second elements to access the encrypted data file from memory when transferring the data file from the memory to the secondary device and to directly re-encrypt the first and second elements when transferring the data file from the secondary device to the memory, wherein the drivers decrypt and re-encrypt the first and second elements using one or more keys generated from identifiers of one or more of the data file, a root directory containing the data file, and a file system containing the root directory. Neither Riedel nor Yu, either alone or in combination, discloses the combination recited in Claim 48, including drivers that decrypt and re-encrypt first and second elements using one or more keys generated from identifiers of one or more of a data file, a root directory containing the data file, and a file system containing the root directory. For at least these reasons, the independent Claim 48 is allowable over Riedel, Yu, and their combination.

The limitation added to Claim 48 finds support throughout the application. Drivers to decrypt and re-encrypt first and second elements using one or more keys generated from identifiers of one or more of a data file, a root directory containing the data file, and a file system containing the root directory, finds support at, for example, page 64, lines 1-8 of the Present Specification.

Claims 49, 50, 68, and 69 all depend on the independent Claim 48. As explained above, the independent Claim 48 is allowable over Riedel, Yu, and their combination. Accordingly, Claims 49, 50, 68, and 69 are all also allowable as depending on an allowable base claim.

Claims 6-8, 14, 15, 29, 38, 39, 51, and 52

Within the Office Action, Claims 6-8, 14, 15, 29, 38, 51, and 52 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to claim 1, and further in view of U.S. Patent Application Pub. No. 2003/0005300 to Noble et al. ("Noble"). The Applicants respectfully disagree.

Claims 6-8, 14, and 15 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 6-8, 14, and 15 are all also allowable as depending on an allowable base claim.

Claim 29 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 29 is also allowable as depending on an allowable base claim.

Claim 38 depends on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claim 38 is also allowable as depending on an allowable base claim.

Claims 51 and 52 both depend on the independent Claim 48. As explained above, the independent Claim 48 is allowable. Accordingly, Claims 51 and 52 are both also allowable as depending on an allowable base claim.

Claim 9

Within the Office Action, Claim 9 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to claim 1, and further in view of Blaze, "A Cryptographic File System for Unix." The Applicants respectfully disagree.

Claim 9 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 9 is also allowable as depending on an allowable base claim.

Claims 10 and 30

Within the Office Action, Claims 10 and 30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu, and further in view of Noble as applied to Claim 5, and further in view of U.S. Patent No. 5,903,881 to Schrader et al. The Applicants respectfully disagree.

Claim 10 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 10 is also allowable as depending on an allowable base claim.

Claim 30 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 30 is also allowable as depending on an allowable base claim.

Claim 13

Within the Office Action, Claim 13 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to Claim 12, and further in view of U.S. Patent No. 5,727,206 to Fish et al. The Applicants respectfully disagree.

Claim 13 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 13 is also allowable as depending on an allowable base claim.

Claims 21, 32, and 44

Within the Office Action, Claims 21, 32, and 44 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to Claim 19, and further in view of U.S. Patent No. 6,836,888 to Basu et al. The Applicants respectfully disagree.

Claim 21 depends on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claim 21 is also allowable as depending on an allowable base claim.

Claim 32 depends on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claim 32 is also allowable as depending on an allowable base claim.

Claim 44 depends on the independent Claim 36. As explained above, the independent Claim 36 is allowable. Accordingly, Claim 44 is also allowable as depending on an allowable base claim.

Claims 22-24, 33-35, 45, and 47

Within the Office Action, Claims 22-24, 33-35, 45, and 47 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to Claim 19, and further in view of U.S. Patent No. 6,477,545 to LaRue. The Applicants respectfully disagree.

Claims 22-24 all depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 22-24 are all also allowable as depending on an allowable base claim.

Claims 33-35, 45, and 47 all depend on the independent Claim 26. As explained above, the independent Claim 26 is allowable. Accordingly, Claims 33-35, 45, and 47 are all also allowable as depending on an allowable base claim.

Claims 59 and 60

Within the Office Action, Claims 59 and 60 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Riedel in view of Yu as applied to Claim 1, and further in view of U.S. Patent No. 6,938,166 to Sarfati et al. ("Sarfati"). The Applicants respectfully disagree.

Claims 59 and 60 both depend on the independent Claim 1. As explained above, the independent Claim 1 is allowable. Accordingly, Claims 59 and 60 are both also allowable as depending on an allowable base claim.

Allowable Subject Matter

Within the Office Action, it is stated that previously pending Claims 16-18, 25, 40, and 41 are objected to and each would be allowable if rewritten in independent form to include the limitations of its corresponding base claim and any intervening claims.

The new independent Claim 74 recites the limitations of the previously pending Claim 16, its independent base claim, Claim 1, and all the intervening claims, Claims 14 and 15, with minor amendments. Where the previously pending Claim 16 incorporated the phrase "to access data contained therein" from the previously pending Claim 1 and further recited "the key engine to use the encrypted data file name key and data file contents," the new independent Claim 74 recites "to access data *file contents* contained therein . . . the key engine to use the encrypted data file name key and *the* data file contents . . . " (italics added). (By way of the above amendments, Claims 1 and 16 have been similarly amended.) These amendments are made to better reflect antecedent basis and do not change the scope of the invention defined in the previously pending Claim 16. Accordingly, Claim 74 is allowable.

The new independent Claim 75 recites the limitations of the previously pending Claim 40 and its independent base claim, Claim 36, the only claim from which it depends, with minor amendments. Where the previously pending Claim 40 recited "the file contents," the new

independent Claim 75 recites "the clear data file." (By way of the above amendments, Claim 40 has been similarly amended.) This language more clearly defines the invention and does not change the scope of the invention defined in the previously pending Claim 40. Accordingly, the new independent Claim 75 is allowable.

Within the Office Action, it is stated that Claims 70, 71 and 73 are allowable.

CONCLUSION

For the reasons given above, the Applicants respectfully submit that Claims 1-45, 47-52 and 59-75 are in condition for allowance, and allowance at an early date would be appreciated. If the Examiner has any questions or comments, the Examiner is encouraged to call the undersigned at (408) 530-9700 so that any outstanding issues can be quickly and efficiently resolved.

Respectfully submitted,
HAVERSTOCK & OWENS LLP

Dated: December 8, 2009

By: /Jonathan O. Owens/
Jonathan O. Owens
Reg. No.: 37,902
Attorneys for Applicants